Nationales Testinstitut für Cybersicherheit

Radio Equipment Directive (RED)

Summarischer Bericht zur Cybersicherheit vernetzter Geräte im Hinblick auf die neue RED-Richtlinie

Version	1.0
Datum	22. Mai 2025
Klassifikation	Öffentlich
Autoren	Tobias Castagna, Patrik Fabian, Andreas Leisibach, Dilip Many, Raphael M. Reischuk, Fabio Zuber
Verantwortlich	Tobias Castagna

Inhaltsübersicht

1 Management Summary

Am 1. August 2025 treten in der Schweiz die neuen Anforderungen der Radio Equipment Directive (RED) (2014/53/EU) in Kraft. Sie legen fest, dass Funkanlagen bestimmte Sicherheits- und Gesundheitsanforderungen erfüllen müssen und betreffen insbesondere die Cybersicherheit von Geräten mit Internetanbindung. Die Anforderungen der RED gelten für nahezu alle Geräte mit einer Funkschnittstelle. Betroffen sind zahlreiche Produktkategorien, darunter IoT-Geräte, vernetzte Fahrzeuge, Industrie 4.0 Anwendungen und Smartphones. Geräte, die ab Inkrafttreten der RED neu auf den Markt gebracht werden, müssen die Anforderungen erfüllen. Bei Nichteinhaltung kann das BAKOM Massnahmen wie z.B. Marktverbote anordnen.

Das NTC hat eine Stichprobe von vernetzten Geräten untersucht. Es handelt sich dabei um im Schweizer Handel häufig verkaufte Produkte der folgenden Kategorien:

- Smartwatches für Kinder
- Babykameras
- Alarmanlagen
- Intelligente Steckdosenadapter
- WLAN-Router

Die Geräte wurden nach einer Auswahl von Anforderungen der RED geprüft, die vom NTC beispielhaft ausgewählt wurde. Dazu gehören die folgenden Anforderungen, die für die Sicherheit und Resilienz der getesteten Geräte von zentraler Bedeutung sind:

- Authentifizierung und Zugriffskontrolle (z.B. Anforderungen an Standardpasswörter)
- Geschützte Datenkommunikation (moderne Verschlüsselungsverfahren)
- Sichere Software-Aktualisierungen (Echtheit und Unversehrtheit von Updates)
- Schutz vor Manipulation und unautorisierten Zugriffen (keine unsichere oder undokumentierte Schnittstellen)

Ein zentrales Ergebnis der NTC-Stichproben: Ein signifikanter Anteil der geprüften Geräte entspricht derzeit nicht den neuen Anforderungen der RED an die Cybersicherheit. Konkrete Beispiele verdeutlichen die Verbreitung dieser Mängel: Alle der getesteten Smartwatches für Kinder sowie eine untersuchte Alarmanlage wiesen eine unzureichende Verschlüsselung bei der Kommunikation mit den Cloud-Plattformen der jeweiligen Hersteller auf. Mehrere der geprüften Babykameras verwendeten unsichere Standardpasswörter; zudem war bei einigen Modellen die lokale Funkübertragung zwischen der Kameraeinheit und der Basisstation nicht ausreichend gegen Abhören geschützt. Die Mehrzahl der geprüften WLAN-Router und intelligenten Steckdosenadapter verwendete zudem keine oder nur eine unzureichende Verschlüsselung für die Kommunikation. Dadurch können sensible Informationen, wie etwa WLAN-Passwörter oder Systemeinstellungen, potenziell mitgelesen werden.

Das NTC sieht einen dringenden Handlungsbedarf für die gesamte Lieferkette – von den Herstellern über die Importeure bis hin zu den Händlern. Um der kommenden Regulierung gerecht zu werden, wird Herstellern empfohlen, die Anforderungen proaktiv umzusetzen, Importeuren und Händlern wird geraten, aktiv Nachweise von ihren Lieferanten einzufordern und Lieferanten sorgfältig auszuwählen. Auch Konsumentinnen und Konsumenten können ebenfalls zu ihrer Sicherheit beitragen, indem sie bei etablierten Händlern in der Schweiz einkaufen, bei Direktimporten vorsichtig sind, Standardpasswörter sofort ändern und regelmässig Updates installieren.

2 Einleitung

Aktuell wird viel über die bevorstehende Einführung neuer EU-Regulierungen wie dem Cyber Resilience Act (CRA) gesprochen, der die Cybersicherheit von Produkten mit digitalen Elementen regelt, oder der NIS2-Richtlinie (Netzwerk- und Informationssystem), die Cybersicherheitsanforderungen für Betreiber kritischer Infrastrukturen festlegt. Diese Richtlinien werden derzeit in den verschiedenen EU-Ländern in nationales Recht umgesetzt. Obwohl die Schweiz als Nicht-EU-Land nicht direkt betroffen ist, müssen Schweizer Unternehmen die Anforderungen ab dem Zeitpunkt der EU-Geltung einhalten, sobald sie in der EU tätig sind.

Neben CRA und NIS2 gibt es eine weitere, oft weniger beachtete Richtlinie: die Radio Equipment Directive (RED) (2014/53/EU). Anders als die zuvor genannten Regelungen wurde diese in der Schweiz in nationales Recht umgesetzt und gilt somit hierzulande für nahezu alle Geräte mit einer Funkschnittstelle. Die Einhaltung wird durch das Bundesamt für Kommunikation (BAKOM) vollzogen.

Die ursprünglich im Jahr 2014 eingeführte RED wurde kontinuierlich erweitert und mit Rechtsakten präzisiert, zuletzt im Jahr 2022, und enthält neue Cybersicherheitsanforderungen, primär für Geräte mit einer Funkschnittstelle, die über das Internet kommunizieren. Die neuen Anforderungen treten am 1. August 2025 in Kraft und gelten für Geräte, die ab diesem Zeitpunkt neu in Verkehr gebracht werden. Betroffen sind zahlreiche Produktkategorien, darunter IoT-Geräte, Geräte für die Kinderbetreuung, Industrie-4.0-Anwendungen und Smartphones.

Interessant ist der breite Anwendungsbereich der RED: So regelt die Richtlinie etwa auch die EU-weite Einführung des universellen USB-C-Ladeanschlusses für Geräte mit Funkkomponenten, darunter Smartphones, Tablets, E-Reader, Digitalkameras, Laptops und Kopfhörer.

Das Nationale Testinstitut für Cybersicherheit NTC hat eine Stichprobe von vernetzten Geräten mit einer Funkschnittstelle im Hinblick auf die neuen Cybersicherheitsanforderungen der Radio Equipment Directive (RED) untersucht. Ziel der Untersuchung ist es, zu bewerten, inwieweit eine Auswahl populärer, in der Schweiz erhältlicher Geräte die neuen Cybersicherheitsanforderungen der RED bereits erfüllt. Zudem sollen typische Schwachstellen identifiziert und der Handlungsbedarf für Hersteller, Importeure, Händler sowie Konsumentinnen und Konsumenten aufgezeigt werden.

Die Analyse zeigt, dass ein Grossteil der getesteten Geräte die neuen Anforderungen an die Cybersicherheit nicht erfüllt. Dies betrifft insbesondere grundlegende Sicherheitsmechanismen wie sichere Authentifizierung, verschlüsselte Kommunikation und Update-Mechanismen. Die Ergebnisse verdeutlichen den Handlungsbedarf sowohl auf Hersteller- als auch auf Vertriebsebene.

Die zentralen Erkenntnisse dieser Untersuchung sind in diesem Bericht zusammengefasst:

- Das Kapitel **"Ausgangslage und Vorgehen"** beschreibt die rechtlichen Rahmenbedingungen der RED sowie die Vorgehensweise der Untersuchung.

- Das Kapitel **" Zusammenfassende Einschätzung "** gibt eine Übersicht über Testresultate der getesteten Geräte, ohne dabei einzelne Geräte oder Hersteller zu benennen und fasst die zentralen Erkenntnisse der Untersuchung zusammen. Basierend darauf enthält das Kapitel konkrete Handlungsempfehlungen für Hersteller, Händler, Importeure sowie Konsumentinnen und Konsumenten.

3 Ausgangslage und Vorgehen

Die Radio Equipment Directive (2014/53/EU) verlangt, dass Funkanlagen bestimmte Sicherheits- und Gesundheitsanforderungen erfüllen. Spezifische neue Anforderungen an die Cybersicherheit, die insbesondere Geräte mit Internetanbindung betreffen, sind in der Delegierten Verordnung (EU) 2022/30 festgelegt, welche die RED ergänzt. Diese neuen Anforderungen werden ab dem 1. August 2025 verbindlich.

Die in Artikel 3.3 (d,e,f) der RED-Richtlinie definierten «RED-Cyber-Anforderungen» werden in den harmonisierten Normen EN 18031-1, EN 18031-2 und EN 18031-3 genauer beschrieben und deren Prüfkriterien definiert. Die Bezeichnung der Normen lautet:

- **EN 18031-1**: Funkanlagen mit Internetanschluss
- **EN 18031-2**: datenverarbeitende Funkanlagen, namentlich mit dem Internet verbundene Funkanlagen, in der Kinderbetreuung eingesetzte Funkanlagen, in Spielzeug eingesetzte Funkanlagen sowie an einem Teil des menschlichen Körpers oder an Kleidungsstücken getragene Funkanlagen
- **EN 18031-3**: mit dem Internet verbundene Funkanlagen, die für die Datenverarbeitung im Zusammenhang mit virtuellen Währungen oder monetären Werten eingesetzt werden

Die Normen definieren zahlreiche sinnvolle Anforderungen, darunter sichere Zugangs- und Authentifizierungsmechanismen, sichere Update- und Speicherverfahren sowie Protokollierungs- und Überwachungsfunktionen.

Das NTC hat eine Stichprobe von 20 vernetzten Geräten untersucht. Es handelt sich dabei um im Schweizer Handel häufig verkaufte Produkte der folgenden Kategorien:

- Mehrere Smartwatches für Kinder (Kategorie EN 18031-2)
- Mehrere Babykameras (Kategorie EN 18031-2)
- Mehrere Alarmanlagen (Kategorie EN 18031-1)
- Mehrere intelligente Steckdosenadapter (Kategorie EN 18031-1)
- Mehrere WLAN-Router (Kategorie EN 18031-1)

Bei der Untersuchung wurden die Geräte nach einer vom NTC bestimmten Auswahl von Anforderungen der RED-Anforderungen überprüft. Die verwendeten Anforderungen aus der RED-Richtlinie umfassen verschiedene sicherheitsrelevante Mechanismen für internetverbundene Funkanlagen. Dazu gehören die folgenden Anforderungen, welche zentral für die Gewährleistung der Sicherheit und Resilienz der getesteten Geräte sind:

Authentifizierung und Zugriffskontrolle: Das Gerät muss sicherstellen, dass nur berechtigte Personen darauf zugreifen können. Standardpasswörter wie „admin" oder „1234", sind dabei nicht erlaubt.

- Beispiel: Ein WLAN-Router sollte bei der ersten Einrichtung ein starkes, individuelles Passwort verlangen oder nicht mit einem leicht zu erratenden Standardpasswort ausgeliefert werden.

Geschützte Datenkommunikation: Datenübertragungen müssen durch moderne Verschlüsselungsverfahren geschützt werden. Dies verhindert das Abhören oder die Manipulation der Daten während der Übertragung.

- Beispiel: Eine Babykamera, die Videos per Funk überträgt, muss eine abhörsichere Verschlüsselung nutzen, um zu verhindern, dass Unbefugte die Übertragung mitverfolgen können.

Sichere Software-Aktualisierungen: Das Gerät darf nur Updates installieren, die nachweislich vom Hersteller stammen und nicht manipuliert wurden. Es braucht Mechanismen, um die Echtheit und Unversehrtheit der Updates zu prüfen.

- Beispiel: Eine Kinder-Smartwatch muss sicherstellen, dass nur geprüfte Updates vom Hersteller installiert werden können, um zu verhindern, dass Schadsoftware auf das Gerät gelangt.

Schutz vor Manipulation und unautorisierten Zugriffen: Es dürfen keine unsicheren oder undokumentierten Schnittstellen vorhanden sein, die Angreifer ausnutzen könnten, um die Kontrolle über das Gerät zu übernehmen.

- Beispiel: Ein intelligenter Steckdosenadapter sollte keine ungesicherten Fernwartungszugänge aktiviert haben, über die Angreifer ohne Passwort eindringen könnten.

Für die Bewertung der Konformität wurden die Geräte einer Prüfung unterzogen, die eine gezielte Auswahl von zehn RED-Anforderungen umfasste. Diese Auswahl repräsentierte etwa einen Drittel des gesamten Anforderungskatalogs der RED. Schon diese reduzierte Prüfungstiefe war ausreichend, um bei einem Grossteil der Geräte Konformitätsmängel festzustellen. Bereits ein einzelner Verstoss gegen eine Anforderung führt dazu, dass das gesamte Gerät als nicht konform gilt und potenziell vom Markt genommen werden muss. Angesichts dessen ist davon auszugehen, dass eine vollumfängliche Prüfung aller RED-Anforderungen zu einer noch höheren Anzahl nicht konformer Geräte geführt hätte.

In diesem Bericht werden bewusst keine spezifischen Produkte oder Hersteller genannt, da der Fokus auf dem allgemeinen Marktbild liegt. Die betroffenen Hersteller wurden vom NTC direkt über die identifizierten Schwachstellen informiert.

4 Zusammenfassende Einschätzung

Die Untersuchungsergebnisse der durchgeführten Stichprobe zeigen, dass ein signifikanter Anteil der getesteten Geräte die neuen Cybersicherheitsanforderungen von RED derzeit nicht erfüllt. Zu den besonders häufig festgestellten Mängeln zählen:

- **Verwendung unsicherer Standard-Anmeldedaten**: Zahlreiche Geräte werden mit leicht erratbaren oder allgemein bekannten Standardpasswörtern (z. B. „admin", „1234") ausgeliefert. Oftmals fehlt ein Mechanismus, der Nutzer bei der ersten Inbetriebnahme zur Änderung dieser unsicheren Zugangsdaten zwingt. Dies stellt eine elementare Schwachstelle dar, da Angreifer so potenziell sehr einfach die Kontrolle über das Gerät erlangen können.

- **Unzureichende Verschlüsselung der Datenkommunikation:** Insbesondere die Übertragung von Daten zwischen dem Gerät und den Cloud-Diensten des Herstellers erfolgte häufig mit ungenügender oder teilweise ohne Verschlüsselung. Dies betrifft potenziell auch sensible Nutzerdaten (z. B. Videoaufnahmen, Standortdaten), die dadurch während der Übertragung für Dritte einsehbar oder manipulierbar werden.

- **Mangelhafte Absicherung der Update-Mechanismen:** Die Prozesse zur Einspielung von Software-Aktualisierungen wiesen bei einigen Geräten gravierende Schwächen auf. Es fehlten grundlegende Prüfungen zur Verifizierung der Integrität und Authentizität der Update-Dateien. Solche Lücken erlauben es Angreifern potenziell, manipulierte oder bösartige Software auf die Geräte aufzuspielen. Darüber hinaus verfügten einzelne Geräte über keinerlei Update-Funktion. Somit können auf diesen Geräten entdeckte Sicherheitslücken nicht nachträglich behoben werden.

Konkrete Beispiele verdeutlichen die Verbreitung dieser Mängel: Alle der getesteten Smartwatches für Kinder sowie eine untersuchte Alarmanlage wiesen eine unzureichende Verschlüsselung bei der Kommunikation mit den Cloud-Plattformen der jeweiligen Hersteller auf. Mehrere der geprüften Babykameras verwendeten unsichere Standardpasswörter; zudem war bei einigen Modellen die lokale Funkübertragung zwischen der Kameraeinheit und der Basisstation nicht ausreichend gegen Abhören geschützt. Die Mehrzahl der geprüften WLAN-Router und intelligenten Steckdosenadapter verwendete zudem keine oder nur eine unzureichende Verschlüsselung für die Kommunikation. Dadurch können sensible Informationen, wie etwa WLAN-Passwörter oder Systemeinstellungen, potenziell mitgelesen werden.

Es ist hervorzuheben, dass die Auswahl der getesteten Geräte statistisch nicht repräsentativ für den gesamten Markt ist. Es wurden jedoch bewusst aktuelle und beliebte Produkte ausgewählt, die im Schweizer Handel erhältlich sind. Die Analyse zeigt, dass Sicherheitsdefizite kein reines Problem von Billigprodukten sind: Auch teurere Geräte etablierter Markenhersteller erfüllen die neuen Anforderungen häufig nicht.

Einige dieser Mängel, wie die Verwendung offensichtlich schwacher Standardpasswörter oder das Ausbleiben einer Aufforderung zur Passwortänderung, sind prinzipiell auch für aufmerksame Konsumentinnen und Konsumenten erkennbar. Viele kritische Schwachstellen, etwa bei der Verschlüsselung oder der Update-Sicherheit, entziehen sich jedoch einer einfachen Überprüfung durch Laien und erfordern technische Expertise.

Aufgrund der Tatsache, dass die verschärften RED-Anforderungen bereits ab dem 1. August 2025 verbindlich für alle neu in Verkehr gebrachten Geräte mit einer Funkschnittstelle gelten, besteht dringender Handlungsbedarf für die gesamte Lieferkette – von den Herstellern über die Importeure bis hin zu den Händlern. Sie alle tragen Verantwortung dafür, sicherzustellen, dass ihre Produkte die gesetzlichen

Sicherheitsvorgaben erfüllen. Das Bundesamt für Kommunikation BAKOM ist zuständig für die Marktüberwachung und kontrolliert die Einhaltung der Vorschriften. Bei Nichteinhaltung kann es Massnahmen wie z.B. Marktverbote anordnen.

Um der kommenden Regulierung gerecht zu werden, wird **Herstellern, Importeuren und Händlern** empfohlen, proaktiv zu handeln:

- **Proaktive Umsetzung und Verifizierung der Sicherheitsanforderungen**: Hersteller sollten die relevanten Cybersicherheitsanforderungen der RED proaktiv und lückenlos in ihren Produkten umsetzen. Dies erfordert, Sicherheit von Beginn an tief in den Entwicklungsprozess zu integrieren ("Security by Design"). Die vollständige Konformität mit allen geforderten Aspekten muss durch umfassende Tests aktiv überprüft und für die Marktzulassung nachgewiesen werden können.

- **Konformität sicherstellen und nachweisen**: Hersteller müssen gewährleisten, dass ihre Produkte die Anforderungen erfüllen. Importeure und Händler sollten aktiv Nachweise von ihren Lieferanten einfordern, dass die Konformitätserklärung explizit die neuen Cybersicherheitsanforderungen (gemäss Art. 3.3 d, e, f der RED) abdeckt.

- **Sorgfalt bei der Lieferantenauswahl**: Eine erhöhte Sorgfalt ist geboten, insbesondere bei Lieferanten ausserhalb der Schweiz und EU. Gegebenenfalls sollten eigene Prüfungen veranlasst oder detaillierte Testberichte verlangt werden, die die Konformität belegen.

Auch **Konsumentinnen und Konsumenten** können zu ihrer Sicherheit beitragen:

- **Bei etablierten Händlern in der Schweiz kaufen**: Diese Händler sind gesetzlich verpflichtet, darauf zu achten, dass die angebotenen Produkte die Schweizer Vorschriften (inklusive RED) erfüllen.

- **Vorsicht bei Direktimporten**: Besonders bei sehr günstigen Angeboten von Online-Plattformen ausserhalb der Schweiz und EU ist das Risiko höher, ein nicht konformes und potenziell unsicheres Gerät zu erhalten. Zudem besteht die Gefahr, dass solche Sendungen bei der Einfuhr vom Zoll gestoppt werden, was für den Käufer Kosten verursachen kann.

- **Standardpasswörter sofort ändern**: Wenn ein Gerät die Möglichkeit bietet, sollte das voreingestellte Passwort bei der ersten Inbetriebnahme in ein starkes, individuelles Passwort geändert werden.

- **Updates installieren**: Die Software der vernetzten Geräte sollte aktuell gehalten werden, sofern der Hersteller Updates anbietet.

Obwohl die bevorstehende Regelung ab August 2025 langfristig zu sichereren Produkten führen soll, lassen die aktuellen Testergebnisse Zweifel aufkommen hinsichtlich einer flächendeckenden und pünktlichen Umsetzung. Es bleibt abzuwarten, wie schnell sich die Marktsituation an die neuen Anforderungen anpasst. Das Nationale Testinstitut für Cybersicherheit NTC wird die Entwicklung weiterhin beobachten und über festgestellte Mängel berichten.